Anand Guru

SECURITY ANALYST

www.linkedin.com/in/anandguru | +1 9876543210 | anandguru.in@gmail.com

TOOLS & TECHNOLOGIES

- IBM QRadar
- Splunk
- IPvoid.com
- VirusTotal.com
- Wireshark
- MXToolbox.com
- Any.run
- Nmap
- Nessus

AREAS OF INTEREST

- Threat Hunting
- Threat Intelligence
- SOAR (IR Automation)
- Malware Analysis
- Forensics

SOMETHING IMP

Use this section to highlight anything special about you, including volunteer work, special projects etc.

EDUCATION

Bachelors - Computer Science

SomeCollege, SomePlace

YearOfPassing

OBJECTIVE

Seeking to further my cybersecurity career by growing with a team where my acquired skills will be utilized for the betterment of the company.

SUMMARY

- 1+ years of experience in Security Operations.
- Solid understanding of common network services and protocols.
- Good knowledge on cyberattacks and attack vectors.
- Working knowledge on security solutions like antivirus, firewall, IPS, Proxy, WAF etc.
- Exposure to using MITRE ATT&CK for threat hunting.
- Good experience working/communicating with cross-functional IT infrastructure

WORK EXPERIENCE

ABC INFO SOLUTIONS
Security Analyst
April 2019 – Till Date

- Monitoring Security alerts generated by SIEM.
- Analyzing SIEM alerts by following runbooks and using various tools.
- Generating tickets for validating incidents.
- Assist in identifying Root Causes of incidents and follow-up with SMEs for incident closure.
- Assist the team lead in generating weekly report.
- Documentation of alerts.
- Draft Shift Handover.